Secure device configuration made simple

GYTPOL

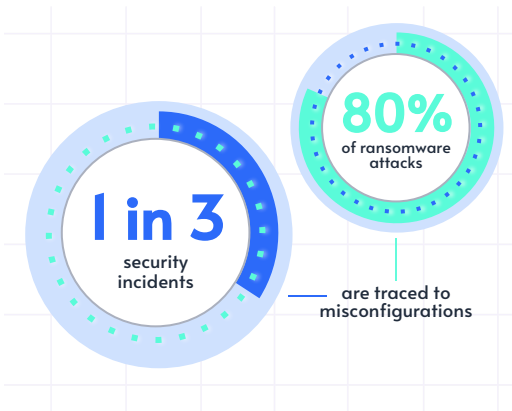
Eliminate blind spots and harden security at the push of a button and with zero risk of disruption.

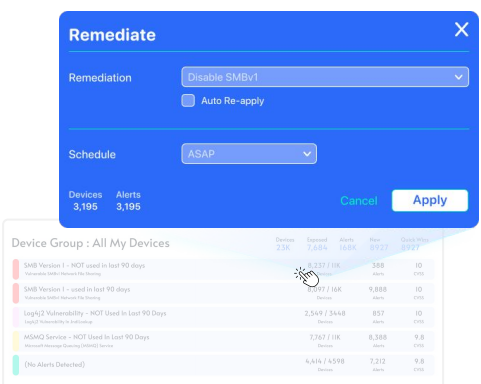
Relied on by

AB InBev · NHS · Carlsberg Group · Check Point · Credit Union · Colgate-Palmolive · UPS · Eaton · Kraft Heinz

Put an end to endpoint misconfigurations

From bad defaults and setup errors to imperfect policy enforcement and non-patchable vulnerabilities, misconfigurations are both common and costly. As a result of operational fragmentation, they also tend to be hard to find and harder to fix.





Detect & correct in one go

Too often remediation is simple in theory, but slow and painful in practice. With GYTPOL it's as simple as pushing a button.

And since GYTPOL maps dependencies, you can make changes with complete confidence and **without fear of breaking things**. As an added fail-safe, any change can be instantly rolled back with a click.

Threat exposure management done right

A continuous and streamlined process

Discover

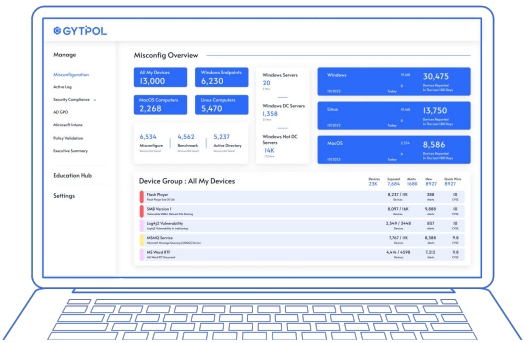
Identify & itemize issues across all device types, operating systems, and security groups

Prioritize

Score and sort issues according to severity, urgency, and other pertinent risk factors

Remediate

Push fixes remotely & dynamically to shrink the attack surface with no risk of disruption



Harden with ease

Deploying in minutes, GYTPOL's detection & correction capabilities extend to:

- Framework compliance (CIS, NIST, etc.)
- Security controls validation
- Device misconfiguration
- Intune, AD, and GPO intelligence
- Browser, web server, and other software risks

CHECK POINT

"GYTPOL gives us compliance, visibility, and remediation for 100% of endpoints and servers. All the time."

Jony Fischbein
Global CISO